Section:	Information Technologies Policies
Policy Name:	Information Classification Policy
Policy Owner:	EVP
Responsible University Office:	Vice President for Information Technologies
Origination Date:	July 1993
Revisions:	October 6, 2005, May 2013, February 26, 2018

I. SCOPE OF POLICY

A. This policy establishes risk-based University information classifications to facilitate institution-wide understanding of data-related risks and implementation of security standards and controls as required by the University Information Security Policy.
B. This policy applies to University information in all forms, including physical and digital, and in all locations, including in storage media, in e-communications, in the cloud, and on personal devices. **Note:** for the purposes of this policy, "University information" does not include an individual's own personal information stored on a computer or device.

II. DEFINITIONS

A. "Availability" means ensuring timely and reliable access to and use of University information.
B. "Confidentiality" means preserving authorized restrictions on University information access and disclosure, including means for protecting personal privacy and proprietary information.
C. "Data set" is a collection of related University information that supports University missions or activities.
D. "Data steward" is an individual within the University who is the primary institutional authority for a particular data set and who is principally responsible for the management and security of that data set across the institution.
E. "Data stewardship" is the responsible oversight of a data set, including principal responsibility for the establishment of standards and guidelines for appropriately managing and securing that data across the institution.
F. "Data trustee" is an executive officer of the University who has the highest level of strategic and policy-setting authority and responsibility for his or her functional area.
G. "End user" is any individual who accesses and/or utilizes IT resources.
H. "Functional area" is one or more units that have primary responsibility for managing a core University mission or business function.
I. "Integrity" means guarding against improper modification or destruction of University information, and includes ensuring non-repudiation and authenticity.

J. “IT resources” are the full set of University owned or controlled information technology devices and data involved in the processing, storage, accessing, and transmission of information.
K. “Security controls” are the administrative, operational, and technical requirements and recommended best practices for meeting security standards.
L. “Security standards” are the requirements for achieving risk management objectives and compliance with laws, regulations, and policies.
M. “Unit” means a University department, school, institute, program, office, initiative, center, or other operating unit.
N. “Unit head” is a University official with the highest level of authority over the day-to-day management or oversight of a unit’s operation.
O. "University information" is defined as any information within the University’s purview, including information that the University may not own but that is governed by laws and regulations to which the University is held accountable. University information encompasses all data that pertains to or supports the administration and missions, including research, of the University.
P. “University information classifications” are the categories of University information that have different security requirements based on their potential impact due to a loss of confidentiality, integrity, or availability.

III. POLICY STATEMENTS

A. University information must be classified according to the University information classifications defined in this policy.
B. University information in all forms and locations must be protected by implementing the administrative, operational, and technical security standards and controls required by its classification.

IV. POLICY STANDARDS AND PROCEDURES

A. This policy establishes three University information classifications based on confidentiality risks:
    1. Level III—High Risk Information
        a. The University is required to implement specific security controls to safeguard the privacy and confidentiality of Level III information as mandated by federal, state and/or local law; University policy; or agreement.
        b. Unintentional, unlawful or unauthorized disclosure of Level III information would have a significant adverse effect on organizational

operations, organizational assets, individuals, other organizations, or the nation.

c. Level III information includes, but is not limited to:
    (1) Confidential information.
    (2) Personally Identifiable Information (PII) - An individual's first name or initial and last name in combination with any of the following:
        i. Social Security number,
        ii. Driver's license number or state-issued ID card number,
        iii. Alien registration or government passport number,
        iv. Account number, or credit or debit card number, in combination with any required security code, access code, PIN or password needed to access an account.
    (3) Protected Health Information (PHI/ePHI) as defined in the Health Insurance Portability and Accountability Act (HIPAA).
    (4) Cardholder Data (CHD) as defined by the Payment Card Industry Data Security Standards (PCI-DSS).
    (5) Export controlled data, including research, subject to the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR).
    (6) Sensitive personally identifiable human subject research.
    (7) UDelNet account passwords or encryption keys used to protect access to Level III information.

d. Data stewards and unit heads may require specific University information not classified as Level III information under this policy to be nonetheless managed according to the same security standards and controls as Level III information. For example, data stewards may require that a data set vital to the operational continuity or effectiveness of the University be protected by the additional security standards prescribed for Level III information, even if that data set does not necessarily carry significant confidentiality risks.

2. Level II—Moderate Risk Information
    a. Level II information includes all University information not categorized as either Level III or Level I.
    b. Level II information refers to official internal records that support the day-to-day operation of University units. This data may sometimes be described as "official use only."
    c. Level II information includes, but is not limited to:
        (1) Student education records, not including directory information, subject to the Family Education Rights Protection Act (FERPA).

(2) Human resources information, such as salary and employee benefits information.
(3) Non-public personal and financial data about applicants and donors.
(4) Information received under grants and contracts subject to confidentiality requirements.
(5) Law enforcement or court records and confidential investigation records.
(6) Citizenship or immigration status.
(7) Unpublished University financial information, strategic plans, and real estate or facility development plans.
(8) Information on facilities security systems.
(9) Nonpublic intellectual property, including unpublished research data, invention disclosures, and patent applications.

3. Level I—Low Risk Information
    a. Level I information is explicitly or implicitly approved for distribution to all members of the University community and to all individuals and entities external to the University community with no legal, regulatory, contractual, or funding agency restrictions on access or usage.
    b. Unintentional, unlawful, or unauthorized disclosure of Level I information would have limited or no adverse effect on organizational operations, organizational assets, individuals, other organizations, or the nation.
    c. Level I information includes, but is not limited to:
        (1) General access data on University websites.
        (2) University financial statements and other reports filed with federal or state governments and generally available to the public.
        (3) Copyrighted materials that are publicly available.
        (4) Directory information under FERPA.

B. Roles and responsibilities
    1. Data trustees
        a. Require the appropriate classification of University information entrusted to their care.
    2. Data stewards
        a. Classify University information within their stewardship according to the three University information classifications:
            (1) Level III—High Risk Information
            (2) Level II—Moderate Risk Information
            (3) Level I—Low Risk Information
        b. Periodically review and update the classifications of University information within their stewardship.

    c. Report to Information Technologies the classifications of University information within their stewardship.
2. Information Technologies
    a. In collaboration with data stewards, develop and maintain a University data dictionary that describes the sets of University information available for access and the University information classifications assigned to them.